Subgroups and cyclic groups

1 Subgroups

In many of the examples of groups we have given, one of the groups is a subset of another, with the same operations. This situation arises very often, and we give it a special name:

Definition 1.1. A *subgroup* H of a group G is a subset $H \subseteq G$ such that

(i) For all $h_1, h_2 \in H$, $h_1 h_2 \in H$.

(ii) $1 \in H$.

(iii) For all $h \in H$, $h^{-1} \in H$.

It follows from (i) that the binary operation $\cdot$ on G induces by restriction a binary operation on H. Moreover, $(H, \cdot)$ is again a group: clearly $\cdot$ remains associative when restricted to elements of H, $1 \in H$ is the identity for H, and for all $h \in H$, the inverse h^{-1} for h viewed as an element of G is an inverse for h in H. We write $H \leq G$ to mean that H is a subgroup of G.

Somewhat informally, one says that H **with the binary operation induced from** G is again a group. This assumes the closure property (i). Note that, if H with the induced operation has **some** identity element, it must automatically be the identity element of G (why?), and if $h \in H$ has an inverse in H, this inverse must be h^{-1}, the inverse for h in G.

Example 1.2. (i) For every group G, $G \leq G$. If $H \leq G$ and $H \neq G$, we call H a *proper subgroup* of G. Similarly, for every group G, $\{1\} \leq G$. We call $\{1\}$ the *trivial subgroup* of G. Most of the time, we are interested in proper, nontrivial subgroups of a group.

(ii) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$; here the operation is necessarily addition. Similarly, $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$, where the operation is multiplication. Likewise, $\mu_n \leq U(1)$, for every n, and $U(1) \leq \mathbb{C}^*$.

(iii) $SO_n \leq O_n \leq GL_n(\mathbb{R})$, and $SO_n \leq SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

(iv) The relation $\leq$ has the following transitivity property: If G is a group, $H \leq G$ (H is a subgroup of G), and $K \leq H$ (K is a subgroup of H), then $K \leq G$. (A subgroup of a subgroup is a subgroup.)

(v) Here are some examples of subsets which are **not** subgroups. For example, $\mathbb{Q}^*$ is **not** a subgroup of $\mathbb{Q}$, even though $\mathbb{Q}^*$ is a subset of $\mathbb{Q}$ and it is a group. Here, if we don't specify the group operation, the group operation on $\mathbb{Q}^*$ is multiplication and the group operation on $\mathbb{Q}$ is addition. But $\mathbb{Q}^*$ is not even closed under addition, nor does it contain the identity in $\mathbb{Q}$ (i.e. 0).

For another example, $\mathbb{Z}/n\mathbb{Z}$ is **not** a subgroup of $\mathbb{Z}$. First, as correctly defined, $\mathbb{Z}/n\mathbb{Z}$ is not even a subset of $\mathbb{Z}$, since the elements of $\mathbb{Z}/n\mathbb{Z}$ are equivalence classes of integers, not integers. We could try to remedy this by simply defining $\mathbb{Z}/n\mathbb{Z}$ to be the set $\{0, 1, \ldots, n-1\} \subseteq \mathbb{Z}$. But the group operation in $\mathbb{Z}/n\mathbb{Z}$ would have to be different than the one in $\mathbb{Z}$. For example, if we make the convention that $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\} \subseteq \mathbb{Z}$, we would have to set $1 + (n-1) = 0$, which is not equal the integer n (in fact n is not even an element of $\mathbb{Z}/n\mathbb{Z}$ as defined).

Another example where subgroups arise naturally is for product groups: For all groups G_1 and G_2, $\{1\} \times G_2$ and $G_1 \times \{1\}$ are subgroups of $G_1 \times G_2$. More generally, if $H_1 \leq G_1$ and $H_2 \leq G_2$, then $H_1 \times H_2 \leq G_1 \times G_2$. However, not all subgroups of $G_1 \times G_2$ are of the form $H_1 \times H_2$ for some subgroups $H_1 \leq G_1$ and $H_2 \leq G_2$.

For example, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is a group with 4 elements:

$$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = \{(0,0), (1,0), (0,1), (1,1)\}.$$

The subgroups of the form $H_1 \times H_2$ are the improper subgroup $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, the trivial subgroup $\{(0,0)\} = \{0\} \times \{0\}$, and the subgroups

$$\{0\} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0), (0,1)\}, \qquad \mathbb{Z}/2\mathbb{Z} \times \{0\} = \{(0,0), (1,0)\}.$$

However, there is one additional subgroup, the "diagonal subgroup"

$$H = \{(0,0), (1,1)\} \subseteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

It is easy to check that H is a subgroup and that H is not of the form $H_1 \times H_2$ for some subgroups $H_1 \leq \mathbb{Z}/2\mathbb{Z}$, $H_2 \leq \mathbb{Z}/2\mathbb{Z}$.

Lemma 1.3. *If H_1 and H_2 are two subgroups of a group G, then $H_1 \cap H_2 \leq G$. In other words, the intersection of two subgroups is a subgroup.*

The proof is an exercise. It is not hard to check that the *union* of two subgroups of a group G is almost never a subgroup: If H_1 and H_2 are two subgroups of a group G, then $H_1 \cup H_2 \leq G \iff$ either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Remark 1.4. Later we shall prove *Cayley's theorem*: If G is a finite group, then there exists an $n \in \mathbb{N}$ such that G is isomorphic to a subgroup of S_n. Thus, the groups S_n contain the information about all finite groups up to isomorphism. Similarly, every finite group is isomorphic to a subgroup of $GL_n(\mathbb{R})$ for some n, and in fact every finite group is isomorphic to a subgroup of O_n for some n. For example, every dihedral group D_n is isomorphic to a subgroup of O_2 (homework).

2 Cyclic subgroups

In this section, we give a very general construction of subgroups of a group G.

Definition 2.1. Let G be a group and let $g \in G$. The *cyclic subgroup generated by* g is the subset

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

We emphasize that we have written down the definition of $\langle g \rangle$ when the group operation is multiplication. If the group operation is written as addition, then we write:

$$\langle g \rangle = \{n \cdot g : n \in \mathbb{Z}\}.$$

To justify the terminology, we have:

Lemma 2.2. *Let G be a group and let $g \in G$.*

(i) *The cyclic subgroup $\langle g \rangle$ generated by g is a subgroup of G.*

(ii) $g \in \langle g \rangle$.

(iii) *If $H \leq G$ and $g \in H$, then $\langle g \rangle \leq H$. Hence $\langle g \rangle$ is the smallest subgroup of G containing g.*

(iv) *$\langle g \rangle$ is abelian.*

Proof. (i) First, $\langle g \rangle$ is closed under the group operation: given two elements of $\langle g \rangle$, necessarily of the form $g^n, g^m \in \langle g \rangle$, by the rules of exponents

$$g^n g^m = g^{n+m} \in \langle g \rangle.$$

Next, $1 = g^0 \in \langle g \rangle$. Finally, if $g^n \in \langle g \rangle$, then $(g^n)^{-1} = g^{-n} \in \langle g \rangle$. Hence $\langle g \rangle \leq G$.

(ii) Clearly $g = g^1 \in \langle g \rangle$.

(iii) If $H \leq G$ and $g \in H$, then $g \cdot g = g^2 \in H$, and by induction

$$g^{n+1} = g \cdot g^n \in H$$

for all $n \in \mathbb{N}$. Since $1 = g^0 \in H$ by definition, and $g^{-n} = (g^n)^{-1} \in H$ for all $n \in \mathbb{N}$, we see that $g^n \in H$ for all $n \in \mathbb{Z}$. Thus $\langle g \rangle \leq H$.

(iv) Given two elements $g^n, g^m \in \langle g \rangle$,

$$g^n g^m = g^{n+m} = g^{m+n} = g^m g^n.$$

Thus $\langle g \rangle$ is abelian. $\square$

Example 2.3. (i) For any group G, $\langle 1 \rangle = \{1\}$ if the operation is multiplication, and $\langle 0 \rangle = \{0\}$ if the operation is addition.

(ii) Note that $\langle g \rangle = \langle g^{-1} \rangle$, since $(g^{-1})^n = g^{-n}$.

(iii) In $\mathbb{Z}$, $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$. For $d \in \mathbb{N}$, $\langle d \rangle = \langle -d \rangle = \{nd : n \in \mathbb{Z}\}$. Thus $\langle d \rangle$ (which is often written as $d\mathbb{Z}$) is the subgroup of $\mathbb{Z}$ consisting of all multiples of d.

(iv) In $\mathbb{Z}/4\mathbb{Z}$, $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}/4\mathbb{Z}$, and $\langle 2 \rangle = \{0, 2\}$ is a nontrivial proper subgroup of $\mathbb{Z}/4\mathbb{Z}$. In $\mathbb{Z}/5\mathbb{Z}$, $\langle 0 \rangle = \{0\}$, and $\langle a \rangle = \mathbb{Z}/5\mathbb{Z}$ for all $a \neq 0$. In $\mathbb{Z}/6\mathbb{Z}$, $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}/6\mathbb{Z}$, and $\langle 2 \rangle = \langle 4 \rangle = \{0, 2, 4\}$ and $\langle 3 \rangle = \{0, 3\}$ are nontrivial proper subgroups of $\mathbb{Z}/6\mathbb{Z}$.

(v) In $\mathbb{R}$, $\langle 2\pi \rangle = \{2n\pi : n \in \mathbb{Z}\}$ is the subset of $\mathbb{R}$ consisting of all integral multiples of 2π; it is sometimes denoted by $2\pi\mathbb{Z}$. More generally, for any $t \in \mathbb{R}$, $\langle t \rangle = \{nt : n \in \mathbb{Z}\}$ is the set of all integral multiples of t.

(vi) In $\mathbb{Q}^*$, $\langle 1 \rangle = \{1\}$ and $\langle -1 \rangle = \{1, -1\}$. On the other hand, $\langle \frac{1}{2} \rangle = \langle 2 \rangle = \{2^n : n \in \mathbb{Z}\}$, which is infinite.

(vii) In $\mathbb{C}^*$, $\langle e^{2\pi i/n} \rangle = \mu_n$.

(viii) In $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, $\langle (0,0) \rangle = \{(0,0)\}$. $\langle (1,0) \rangle = \{(0,0), (1,0)\}$. $\langle (0,1) \rangle = \{(0,0), (0,1)\}$. $\langle (1,1) \rangle = \{(0,0), (1,1)\}$.

To better get a sense of what the cyclic subgroup $\langle g \rangle$ looks like in general, we divide up into two cases:

Case I: g has infinite order. In this case, we claim that $g^n = g^m \iff n = m$. Clearly, if $n = m$, then $g^n = g^m$. Conversely, suppose that $g^n = g^m$. Now either $n \leq m$ or $m \leq n$. By symmetry, we can suppose that $m \leq n$. Then, since $g^n = g^m$, $g^n(g^m)^{-1} = 1$. But then $g^n(g^m)^{-1} = g^n g^{-m} = g^{n-m} = 1$. Then $n - m \geq 0$, but $n - m > 0$ is impossible since g^k is never 1 for a positive integer k. Thus $n - m = 0$, i.e. $n = m$. In particular, we see that $\langle g \rangle$ is infinite (and hence that G is infinite).

There is a more precise statement:

Proposition 2.4. *Suppose that $g \in G$ has infinite order. Then $\langle g \rangle \cong \mathbb{Z}$.*

Proof. Define $f \colon \mathbb{Z} \to \langle g \rangle$ by $f(n) = g^n$. The discussion above shows that f is injective, since $f(n) = f(m) \iff g^n = g^m \iff n = m$. By the definition of $\langle g \rangle$, f is surjective. Thus f is a bijection. Finally, by the rules of exponents,

$$f(n + m) = g^{n+m} = g^n g^m = f(n)f(m).$$

Thus f is an isomorphism. $\square$

Case II: g has finite order n. In this case, we claim that the elements $1 = g^0, g = g^1, g^2, \ldots, g^{n-1}$ are all different. As before, we suppose that $g^a = g^b$ with $0 \leq a, b \leq n - 1$. By symmetry we can assume that $a \leq b$. Then $1 = g^b(g^a)^{-1} = g^{b-a}$. But $0 \leq b - a \leq b \leq n - 1 < n$. Since the order of g is n, no smaller positive power of g is the identity, so that we must have $b - a = 0$, i.e. $a = b$.

Thus the powers $1, g, g^2, \ldots, g^{n-1}$ are all different. Then $g^n = 1$, $g^{n+1} = g^n g = g$, $g^{n+2} = g^n g^2 = g^2, \ldots$. In other words, the sequence of powers cycles back over the same values. Moreover, $g^{n-1} = g^{-1}$, $g^{n-2} = g^{-2}$, and so the negative powers of g look like $g^{-n} = 1, g^{-(n-1)} = g^{-n+1} = g, \ldots, g^{-2} = g^{n-2}, g^{-1} = g^{n-1}$. In other words, the sequence of powers looks the same in the negative direction as well. From this it is easy to see that $\#(\langle g \rangle) = n$, in other words that the order of an element of finite order is the same as the order of the cyclic subgroup that it generates, connecting the two different meanings of the word order.

We will prove all of this more carefully soon, but we will just state the main result now:

Proposition 2.5. *Suppose that $g \in G$ has order n. Then:*

(i) *$\#(\langle g \rangle) = n$, and $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$.*

(ii) $g^N = 1 \iff n$ *divides* N.

(iii) $\langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

Definition 2.6. A group G is a *cyclic group* if there exists a $g \in G$ such that $G = \langle g \rangle$. In this case, g is called a *generator* of G.

For example, $\mathbb{Z}$ is cyclic; the possible generators are 1 and -1. $\mathbb{Z}/n\mathbb{Z}$ is cyclic; 1 and -1 are generators, but there may be others. μ_n is cyclic; $e^{2\pi i/n}$ is a generator.

However, most groups are **not** cyclic. For example, we have seen that every cyclic group is abelian, so that a non-abelian group is not cyclic. Also, if G is a cyclic group, then either G is finite or there is an isomorphism from $\mathbb{Z}$ to G, hence a bijection from $\mathbb{Z}$ to G. Infinite sets X for which there exists a bijection from $\mathbb{Z}$ to X are called *countable* (because there also exists a bijection from $\mathbb{N}$ to X). For example, $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are countable, but $\mathbb{R}$ and $\mathbb{C}$ are not. Thus, just by a counting argument, $\mathbb{R}$ and $\mathbb{C}$ are not cyclic groups. It is not hard to show that $\mathbb{Q}$ is not cyclic (homework), and a similar method shows that $\mathbb{R}$ and $\mathbb{C}$ are not cyclic without using counting properties of infinite sets. For an example of a finite abelian group which is not cyclic, consider $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. We have listed the cyclic subgroups of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ corresponding to all possible elements of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, and none of these is equal to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Thus $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is not cyclic. There is the following easy criterion for when a finite group is cyclic:

Lemma 2.7. *Let G be a finite group with $\#(G) = n$. Then G is cyclic $\iff$ there exists a $g \in G$ such that the order of g is n.*

Proof. We use the fact mentioned above, which we shall prove carefully later, that, if the order of g is n, then $\#(\langle g \rangle) = n$. So, if G is cyclic, say $G = \langle g \rangle$, then

$$n = \#(G) = \#(\langle g \rangle),$$

and hence the order of g is n. Conversely, if the order of g is n, then $\#(\langle g \rangle) = n$. Since $\langle g \rangle \subseteq G$ and they both have the same number of elements, we must have $\langle g \rangle = G$, and therefore G is cyclic. $\square$

Finally, we say a few words about the subgroups of a group G generated by more than one element. Given a group G and elements $g_1, \ldots, g_k \in G$, we can define the *subgroup generated by* $g_1, \ldots, g_k$ to be the smallest subgroup of G containing $g_1, \ldots, g_k$. We will write this subgroup as $\langle g_1, \ldots, g_k \rangle$. However, if G is not abelian, then there is no simple description of the elements

of $\langle g_1, \ldots, g_k \rangle$. The most that we can say is that every element looks like a product $g_{a_1}^{n_1} \cdots g_{a_t}^{n_t}$ of powers of the elements $g_1, \ldots, g_k$, where the a_i are just some elements in $\{1, \ldots, k\}$ and t can be arbitrarily large in some examples. Here we can take all powers n_i to be ± 1 by allowing repeats, i.e. by letting $g_{a_i} = g_{a_{i+1}}$ as needed. In general, we don't know if any simplification is possible. However, if G is **abelian**, or more generally if the g_i commute with each other (i.e. for all i, j with $1 \leq i, j \leq k$, $g_i g_j = g_j g_i$), then it is easy to check that

$$\langle g_1, \ldots, g_k \rangle = \{g_1^{n_1} \cdots g_k^{n_k} : n_1, \ldots, n_k \in \mathbb{Z}\}$$

is a subgroup of G and it is the smallest subgroup of G containing $g_1, \ldots, g_k$. This should look more familiar if we write the operation on G as $+$, so that G is abelian by convention. Then

$$\langle g_1, \ldots, g_k \rangle = \{(n_1 \cdot g_1) + \cdots + (n_k \cdot g_k) : n_1, \ldots, n_k \in \mathbb{Z}\}.$$

Thus, the group generated by $g_1, \ldots, g_k$ is analogous to the span of k vectors in linear algebra.